

Harold M. Edwards

# Galois Theory



Springer-Verlag

New York Berlin Heidelberg London Paris  
Tokyo Hong Kong Barcelona Budapest

Harold M. Edwards  
New York University  
Courant Institute of  
Mathematical Sciences  
251 Mercer Street  
New York, NY 10012  
USA

*Editorial Board*

J.H. Ewing  
Department of  
Mathematics  
Indiana University  
Bloomington, IN 47405  
USA

F.W. Gehring  
Department of  
Mathematics  
University of Michigan  
Ann Arbor, MI 48109  
USA

P.R. Halmos  
Department of  
Mathematics  
Santa Clara University  
Santa Clara, CA 95053  
USA

---

AMS Classifications: 12-01, 12-03, 12A55, 01A55

---

Library of Congress Cataloging in Publication Data  
Edwards, Harold M.

Galois theory.  
(Graduate texts in mathematics; 101)

Bibliography: p.

Includes index.

1. Galois theory. I. Title. II. Series.  
QA247.E383 1984 512'.32 83-20082

Printed on acid free paper.

© 1984 by Harold M. Edwards

All rights reserved. No part of this book may be translated or reproduced in any form without written permission from the copyright holder.

Typeset by Composition House Ltd., Salisbury, England.  
Printed and bound by R. R. Donnelley & Sons, Harrisonburg, VA.  
Printed in the United States of America.

9 8 7 6 5 4 3 2 (corrected second printing, 1993)

ISBN 0-387-90980-X Springer-Verlag New York Berlin Heidelberg  
ISBN 3-540-90980-X Springer-Verlag Berlin Heidelberg New York

# Contents

Acknowledgments xiii

§1. Galois §2. Influence of Lagrange §3. Quadratic equations §4. 1700 B.C. to A.D. 1500 §5. Solution of cubic §6. Solution of quartic §7. Impossibility of quintic §8. Newton §9. Symmetric polynomials in roots §10. Fundamental theorem on symmetric polynomials §11. Proof §12. Newton's theorem §13. Discriminants  
First Exercise Set 13

§14. Solution of cubic §15. Lagrange and Vandermonde §16. Lagrange resolvents §17. Solution of quartic again §18. Attempt at quintic §19. Lagrange's *Réflexions*  
Second Exercise Set 22

§20. Cyclotomic equations §21. The cases  $n = 3, 5$  §22.  $n = 7, 11$  §23. General case §24. Two lemmas §25. Gauss's method §26.  $p$ -gons by ruler and compass §27. Summary  
Third Exercise Set 31

§28. Resolvents §29. Lagrange's theorem §30. Proof §31. Galois resolvents §32. Existence of Galois resolvents §33. Representation of the splitting field as  $K(t)$  §34. Simple algebraic extensions §35. Euclidean algorithm §36. Construction of simple algebraic extensions §37. Galois' method  
Fourth Exercise Set 45

§38. Review §39. Finite permutation groups §40. Subgroups, normal subgroups §41. The Galois group of an equation §42. Examples  
Fifth Exercise Set 56

§43. Solvability by radicals §44. Reduction of the Galois group by a cyclic extension §45. Solvable groups §46. Reduction to a normal subgroup of index  $p$  §47. Theorem on solution by radicals (assuming roots of unity) §48. Summary  
Sixth Exercise Set 65

§49. Splitting fields §50. Fundamental theorem of algebra (so-called) §51. Construction of a splitting field §52. Need for a factorization method §53. Three theorems on factorization methods §54. Uniqueness of factorization of polynomials §55. Factorization over  $\mathbb{Z}$  §56. Over  $\mathbb{Q}$  §57. Gauss's lemma, factorization over  $\mathbb{Q}$  §58. Over transcendental extensions §59. Of polynomials in two variables §60. Over algebraic extensions §61. Final remarks  
Seventh Exercise Set 81

§62. Review of Galois theory §63. Fundamental theorem of Galois theory (so-called) §64. Galois group of  $x^p - 1 = 0$  over  $\mathbb{Q}$  §65. Solvability of the cyclotomic equation §66. Theorem on solution by radicals §67. Equations with literal coefficients §68. Equations of prime degree §69. Galois group of  $x^n - 1 = 0$  over  $\mathbb{Q}$  §70. Proof of the main proposition §71. Deduction of Lemma 2 of §24  
Eighth Exercise Set 97

Appendix 1. Memoir on the Conditions for Solvability of Equations by Radicals, by Evariste Galois	101
Appendix 2. Synopsis	114
Appendix 3. Groups	118
Answers to Exercises	123
List of Exercises	145
References	149
Index	151